(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－338993

(43)公開日　平成11年(1999)12月10日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｋ　19/073		Ｇ０６Ｋ　19/00	Ｐ
19/10			Ｒ

審査請求　未請求　請求項の数６　ＯＬ　（全 10 頁）

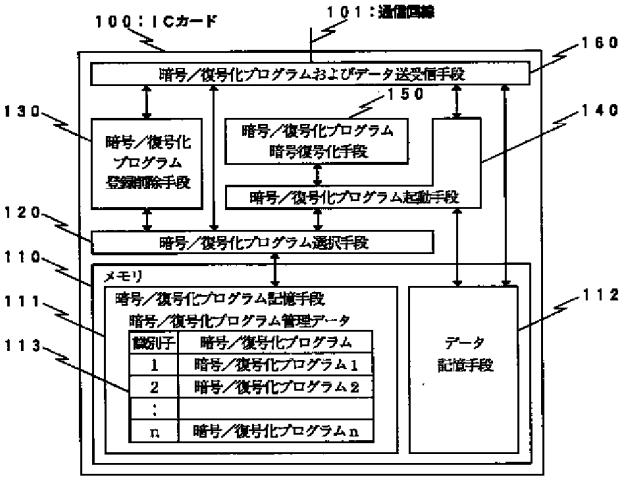
(21)出願番号　特願平10－149147

(22)出願日　平成10年(1998) 5 月29日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　尾花　学
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内
(72)発明者　奥原　進
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内
(72)発明者　竹藪　英樹
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内
(74)代理人　弁理士　矢島　保夫

(54)【発明の名称】　ＩＣカード

(57)【要約】
【課題】プログラムに基づいた暗号および復号処理により送受信データを暗号化および復号化してＩＣカードにデータを送受信するシステムにおいて、ＩＣカード毎に異なる暗号化および復号化プログラムを使用することを容易にすると共に、ＩＣカードへの送受信データの秘匿性の向上を可能にする。
【解決手段】送受信対象となるデータの暗号化および復号化を行なうプログラム（暗号／復号化プログラム）をＩＣカード内に複数に記憶させる手段、任意の暗号／復号化プログラムを選択する手段、暗号／復号化プログラムを登録削除する手段、暗号／復号化プログラムを起動して送受信データを暗号あるいは復号化する手段、暗号／復号化プログラム自体を別の暗号／復号化プログラムで暗号化または復号化するための手段および暗号／復号化プログラムを送受信するための手段を備えたＩＣカード。



1

【特許請求の範囲】

【請求項１】プログラムに基づいた暗号および復号処理により送受信データを暗号化するシステムで用いるＩＣカードであって、

暗号化あるいは復号化プログラム（以後、暗号／復号化プログラムと記述する）を記憶するための暗号／復号化プログラム記憶手段と、

暗号／復号化プログラム記憶手段に記憶された暗号／復号化プログラムを起動させ、暗号化対象データを暗号データとし、または、復号化対象データを復号データとする、暗号／復号化プログラム起動手段と、

暗号／復号化プログラムにより暗号化したデータを送信するときに、データ受信元に対して事前にまたは同時に、暗号化したデータを解読するための暗号／復号化プログラムを送信および受信する暗号／復号化プログラム送受信手段と、

暗号／復号化プログラム記憶手段に対して暗号／復号化プログラムを登録および削除する暗号／復号化プログラム登録削除手段とを備えたことを特徴とするＩＣカード。

【請求項２】前記暗号／復号化プログラム記憶手段は、前記暗号／復号化プログラムを複数記憶することを特徴とする請求項１に記載のＩＣカード。

【請求項３】請求項２に記載の暗号／復号化プログラム記憶手段を備えるＩＣカードにおいて、複数の暗号／復号化プログラムから任意の暗号／復号化プログラムを登録および削除する手段と、更に暗号／復号化プログラム起動手段において任意の暗号／復号化プログラムを起動する暗号／復号化プログラム選択手段を備えた請求項２に記載のＩＣカード。

【請求項４】請求項３に記載の暗号／復号化プログラム選択手段において、ＩＣカード内に記憶されている任意の暗号／復号化プログラムを識別するための識別手段を備え、識別子を指定することで、対応する暗号／復号化プログラムを起動する暗号／復号化プログラム起動手段を備えた請求項３に記載のＩＣカード。

【請求項５】請求項１に記載した暗号／復号化プログラム自体を別の暗号化鍵または暗号化プログラムで暗号化する手段と、暗号化されたプログラムを暗号化した暗号化鍵に対応する復号化鍵または復号化プログラムで復号化する暗号／復号化プログラム暗号復号化手段を備えた請求項１から４の何れか１つに記載のＩＣカード。

【請求項６】請求項１から５の何れか１つに記載のＩＣカード、並びに、該ＩＣカードに対して通信回線を介して任意の暗号／復号プログラムを送信する手段と、送信した暗号／復号化プログラムのＩＣカード内への登録要求手段と、ＩＣカード内の任意の暗号／復号化プログラムの削除要求手段とを備えた情報処理装置を使用して、ＩＣカードと情報処理装置間、または異なるＩＣカード間で、通信回線を介して送受信するデータの暗号化および復号化を行なうことを特徴とする暗号／復号化システム。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、プログラムに基づいた暗号および復号処理によりデータを暗号化および復号化するＩＣカードに関する。

【０００２】

【従来の技術】従来、データ（「情報」とも言う。）を秘匿するための手法として、暗号化鍵を用いて秘匿したいデータを暗号化する処理が知られている。データが一旦暗号化されると、暗号化で使用した鍵と同一の鍵あるいは特定の復号化鍵を使用しないと解読できる状態に戻すことはできないため、そのような暗号化鍵や復号化鍵を所有していない人に対してデータを秘密にすることが可能である。

【０００３】さらに、暗号化鍵や復号化鍵が漏洩すればデータが解読されてしまうことから、この暗号化鍵や復号化鍵に対して別の暗号化鍵にて暗号化して保管することにより安全性を高めてきた。

【０００４】このようなシステムにおいてデータの暗号化処理あるいはデータ解読のための復号化処理は、情報処理装置にて暗号／復号化プログラムにより実行されるのが一般的である。この暗号／復号化プログラムによりデータが暗号化され、更に安全性を高めるために暗号化鍵まで暗号化することで、データの秘匿性を高めている。しかし、この暗号／復号化プログラム自体は、データ自体よりも無防備である事が多い。もしこのような暗号／復号化プログラムが第三者により解析されると、暗号化されたデータが解読されてしまう。または暗号／復号化プログラム自体を改竄し、第三者の知っている暗号化鍵にて暗号化する手段を付加することにより、その後、暗号化されたすべてのデータを第三者が解読することが可能になる恐れもある。

【０００５】この暗号／復号化プログラムを第三者に改竄されることなく、かつ暗号化あるいは復号化を効率的に行うために、特開平９－６２３２号では、暗号／復号化プログラム自体を別の暗号化鍵で暗号化し、情報処理装置内の不揮発性メモリに格納し、情報処理装置からＩＣカードに対してデータを送信する際に、暗号化された暗号／復号化プログラムをＩＣカード内の揮発性メモリに送信し、ＩＣカード内において当該プログラムを復号化した後に情報処理装置の揮発性メモリに送信し、復号化された暗号／復号化プログラムを用いて、送信するデータの暗号化あるいは復号化を行なっている。

【０００６】

【発明が解決しようとする課題】しかし、このようなシステムにおいて、各ＩＣカード毎に異なる暗号／復号化プログラムを使用する場合は、ＩＣカードとデータを送受信する情報処理装置内に全てのＩＣカードの暗号化さ

れた暗号／復号化プログラムを保有する必要があるため、膨大な記憶容量が要求されるという課題があった。

【０００７】さらにＩＣカード内で復号化した暗号／復号化プログラムを情報処理装置に送信する際、暗号／復号化プログラムは無防備な状態であり、送信中の暗号／復号化プログラムの漏洩の可能性が拡大するという課題がある。

【０００８】本発明は、全てのＩＣカードの暗号／復号化プログラムを情報処理装置内に一括保有する必要が無く、暗号／復号化プログラムの秘匿性を向上させたＩＣカードを提供することを目的とする。

【０００９】

【課題を解決するための手段】上記目的を達成するため、本発明は、暗号／復号化プログラムを記憶させる手段と、暗号／復号化プログラムを起動させる手段と、暗号／復号化プログラム自体を外部の情報処理装置または他のＩＣカードに送受信する手段と、暗号／復号化プログラム登録削除手段をＩＣカード内に備えることを特徴とする。

【００１０】すなわち、請求項１に係る発明は、プログラムに基づいた暗号および復号処理により送受信データを暗号化するシステムで用いるＩＣカードであって、暗号化あるいは復号化プログラム（以後、暗号／復号化プログラムと記述する）を記憶するための暗号／復号化プログラム記憶手段と、暗号／復号化プログラム記憶手段に記憶された暗号／復号化プログラムを起動させ、暗号化対象データを暗号データとし、または、復号化対象データを復号データとする、暗号／復号化プログラム起動手段と、暗号／復号化プログラムにより暗号化したデータを送信するときに、データ受信元に対して事前にまたは同時に、暗号化したデータを解読するための暗号／復号化プログラムを送信および受信する暗号／復号化プログラム送受信手段と、暗号／復号化プログラム記憶手段に対して暗号／復号化プログラムを登録および削除する暗号／復号化プログラム登録削除手段とを備えたことを特徴とする。

【００１１】請求項２に係る発明は、請求項１において、前記暗号／復号化プログラム記憶手段は、前記暗号／復号化プログラムを複数記憶することを特徴とする。

【００１２】請求項３に係る発明は、請求項２に記載の暗号／復号化プログラム記憶手段を備えるＩＣカードにおいて、複数の暗号／復号化プログラムから任意の暗号／復号化プログラムを登録および削除する手段と、更に暗号／復号化プログラム起動手段において任意の暗号／復号化プログラムを起動する暗号／復号化プログラム選択手段を備えたことを特徴とする。

【００１３】請求項４に係る発明は、請求項３に記載の暗号／復号化プログラム選択手段において、ＩＣカード内に記憶されている任意の暗号／復号化プログラムを識別するための識別手段を備え、識別子を指定することで、対応する暗号／復号化プログラムを起動する暗号／復号化プログラム起動手段を備えたことを特徴とする。

【００１４】請求項５に係る発明は、請求項１～４において、請求項１に記載した暗号／復号化プログラム自体を別の暗号化鍵または暗号化プログラムで暗号化する手段と、暗号化されたプログラムを暗号化した暗号化鍵に対応する復号化鍵または復号化プログラムで復号化する暗号／復号化プログラム暗号復号化手段を備えたことを特徴とする。

【００１５】請求項６に係る発明は、請求項１から５の何れか１つに記載のＩＣカード、並びに、該ＩＣカードに対して通信回線を介して任意の暗号／復号プログラムを送信する手段と、送信した暗号／復号化プログラムのＩＣカード内への登録要求手段と、ＩＣカード内の任意の暗号／復号化プログラムの削除要求手段とを備えた情報処理装置を使用して、ＩＣカードと情報処理装置間、または異なるＩＣカード間で、通信回線を介して送受信するデータの暗号化および復号化を行なうことを特徴とする暗号／復号化システムである。

【００１６】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態を説明する。

【００１７】図２は、本発明の実施の形態のＩＣカード１００を構成するハード機構ブロック図である。このＩＣカード１００は、ＣＰＵ２１０、入出力インタフェース（Ｉ／Ｏ）２２０、ＲＯＭ２３０、ＲＡＭ２５０、およびＥＥＰＲＯＭ２４０を備えている。ＲＯＭ２３０は、記憶内容の読み出しは可能であるが記憶内容の更新ができない不揮発性のメモリを示す。ＲＡＭ２５０およびＥＥＰＲＯＭ２４０は、共に記憶内容の読み出しならびに更新が可能であるが、ＲＡＭ２５０はＩＣカード１００への電源供給が断たれると記憶内容を失う揮発性のメモリを示し、ＥＥＰＲＯＭ２４０はＩＣカード１００への電源供給が断たれても記憶内容を失わない不揮発性のメモリを示す。

【００１８】図１は、図２に示すＩＣカード１００内に本発明を実現するための各構成要素を配置したブロック図である。メモリ１１０は、図２のＲＡＭ２５０またはＥＥＰＲＯＭ２４０内に割り当てられた記憶領域を示す。秘密にしたいデータを暗号化あるいは暗号化されたデータを復号化するための暗号／復号化プログラムを記憶する暗号／復号化プログラム記憶手段１１１は、メモリ１１０内に割り当てられる。

【００１９】また、ＩＣカード１００が受信したデータまたはＩＣカード１００内で処理するデータを記憶するためのデータ記憶手段１１２を、メモリ１１０内の暗号／復号化プログラム記憶手段１１１とは別の領域に割り当てる。

【００２０】暗号／復号化プログラム記憶手段１１１内に記憶されている各暗号／復号化プログラムは、暗号／

復号化プログラム管理データ１１３によって管理する。図９は、暗号／復号化プログラム管理データの一実施例である。

【００２１】ＩＣカード１００内の処理で任意の暗号／復号化プログラムを選択する場合、暗号／復号化プログラム選択手段１２０が暗号／復号化プログラム管理データ１１３を参照することで、指定された暗号／復号化プログラムを選択する。

【００２２】任意の暗号／復号化プログラムを暗号／復号化プログラム記憶手段１１１に登録または暗号／復号化プログラム記憶手段１１１に既に登録されている任意の暗号／復号化プログラムを削除する場合、指定された暗号／復号化プログラムを暗号／復号化プログラム選択手段１２０により選択した結果を元に、暗号／復号化プログラム登録削除手段１３０によって暗号／復号化プログラム記憶手段１１１内の暗号／復号化プログラム管理データ１１３に管理データを登録すると共に指定された暗号／復号化プログラムをメモリ１１０内に組込む、または暗号／復号化プログラム管理データ１１３から対応する管理データを削除すると共に対応する暗号／復号化プログラムをメモリ１１０から削除する。

【００２３】任意の暗号／復号化プログラムをＩＣカード１００内で起動する場合は、指定された暗号／復号化プログラムを暗号／復号化プログラム選択手段１２０により選択した結果を元に、暗号／復号化プログラム起動手段１４０によって指定された暗号／復号化プログラムを起動することで、データ記憶手段１１２内に記憶されている暗号化すべきデータの暗号化または復号化を行なう。

【００２４】暗号／復号化プログラム起動手段１４０において、指定された暗号／復号化プログラムの暗号／復号化プログラム管理データ１１３内に暗号／復号化プログラム自体の復号化が必要なデータが格納されていた場合は、暗号／復号化プログラム暗号復号化手段１５０で指定された暗号／復号化プログラムを復号化してから暗号／復号化プログラム起動手段１４０によって起動する。

【００２５】ＩＣカード１００において外部の情報処理装置からデータあるいは暗号／復号化プログラムを受信、または外部の情報処理装置にデータあるいは暗号／復号化プログラムを送信する場合は、暗号／復号化プログラムおよびデータ送受信手段１６０によって入出力インタフェース（Ｉ／Ｏ）２２０を使用して通信回線１０１へのデータの送受信を行う。

【００２６】図１のブロック図において、暗号／復号化プログラム選択手段１２０、暗号／復号化プログラム登録削除手段１３０、暗号／復号化プログラム起動手段１４０、暗号／復号化プログラム暗号復号化手段１５０、並びに、暗号／復号化プログラムおよびデータ送受信手段１６０は、ＩＣカード１００内の不揮発性メモリであるＲＯＭ２３０またはＥＥＰＲＯＭ２４０内に組込む。

【００２７】以後、図１および図２に示した実施の形態のＩＣカード１００を使用した暗号化および暗号化データ転送の一例を、図３～９に基づいて説明する。

【００２８】図３は、ＩＣカード１００の入出力インタフェース（Ｉ／Ｏ）２２０を使用して通信回線１０１にデータ送信、または通信回線１０１からデータを受信するための暗号／復号化プログラムおよびデータ送受信手段１６０の処理を示す。本処理は、ＩＣカード１００が実行状態のときは常にデータ送受信の受付けを可能にするため、Ｓ３１０およびＳ３３０の判定処理によって送受信データの有無の監視を行なう。

【００２９】図８に、送受信するデータの形式を示す。受信データが有るときは、Ｓ３４０の処理で、受信データのヘッダー部のデータ種別を判定する。データ種別は、暗号化プログラム、復号化プログラム、またはデータであることを判定するための情報が設定されている。暗号／復号化プログラムならば、Ｓ３５０処理において受信データから暗号／復号化プログラムの識別子を読取り、Ｓ４００処理で指定識別子に対応する暗号／復号化プログラムの有無を確認する。

【００３０】図４に、Ｓ４００の暗号／復号化プログラム選択処理の流れを示す。暗号／復号化プログラム選択処理Ｓ４００では、ＥＥＰＲＯＭ２４０とＲＡＭ２５０内に設定されている暗号／復号化プログラム管理データ１１３から、受信した暗号／復号化プログラムの識別子と一致する識別子を検索する。対応する識別子が検出された場合は（Ｓ４２０）、その識別子に対応する暗号／復号化プログラム管理データをリターンし、検出できなかった場合は未登録としてエラーコードを設定して、Ｓ４００処理コール元へリターンする。

【００３１】Ｓ４００処理で検索対象になる暗号／復号化プログラム管理データ１１３は、図９に示すような形式を構成している。暗号／復号化プログラムを識別するための識別子は、暗号／復号化プログラムを登録したカードＩＤとそのカード内で管理している暗号／復号化プログラムの番号から構成される。暗号／復号化プログラムの管理データは、暗号化プログラムのＩＣカード１００内の格納アドレス、ＩＣカード１００内の復号化プログラムの格納アドレス、そしてＩＣカード１００内に登録されているメモリ種別（ＥＥＰＲＯＭまたはＲＡＭの別）、および登録されている暗号／復号プログラムを実行する前に暗号／復号化プログラム自体を復号化する必要がある場合は、その復号化に使用する暗号／復号化プログラムの識別子（復号処理の欄）から構成されている。

【００３２】図９に示した例では、自ＩＣカード１００のカードＩＤを「Ｃ００１」とすると、自ＩＣカードで登録した暗号／復号化プログラム識別子は「Ｃ００１０１」「Ｃ００１０２」の２種類であり（識別子は登録カ

ードＩＤとＮｏをつなげて表すものとする）、識別子が「Ｃ００１０２」である暗号／復号化プログラムは「Ｃ００１０１」によって暗号化されていることを表わしている。また暗号／復号化プログラム識別子「Ｃ０２０１０」は、カードＩＤ「Ｃ０２０」からのデータ受信時にデータを復号化するための復号化プログラムの管理データのみが格納されていることを表す。さらに、暗号／復号化プログラム識別子「Ｃ０００００」は、全ＩＣカード共通に使用できるように、標準的にＩＣカード１００内に登録した暗号／復号化プログラムを表す。暗号／復号化プログラム識別子「Ｃ００１０１」や「Ｃ０３０１１」は、この標準登録された「Ｃ０００００」で暗号化されていることを表している。

【００３３】再び図３に戻って、暗号／復号化プログラムおよびデータ送受信処理Ｓ３００のＳ４００処理で検索した結果を元に、Ｓ３６０処理で、受信データヘッダー部より受信した暗号／復号化プログラムを登録するか削除するかを判定する。削除要求の場合は、暗号/復号化プログラム削除処理Ｓ５００をコールして、指定暗号／復号化プログラムを削除した後、送信データの有無をチェックするＳ３１０から繰り返し処理を実行する。登録要求の場合は、Ｓ４００処理の結果を元に、Ｓ３７０処理で受信した暗号／復号化プログラムが既に登録されているか判定し、未登録の場合は、暗号／復号化プログラム登録処理Ｓ５００をコールする。Ｓ３７０処理で指定暗号／復号化プログラムが既に登録されていた場合、またはＳ５００処理で新規に暗号／復号化プログラムをメモリ１１０内に登録した場合は、引き続き指定した暗号／復号化プログラム起動処理Ｓ６００をコールし、引き続き、ＩＣカード１００が受信するデータの復号化処理を実行する。

【００３４】Ｓ６００処理で復号化されたデータは、Ｓ３８０処理で受信データを加工し、メモリ１１０に記憶させるなどの処理を実行した後、Ｓ３１０処理から繰り返し実行する。

【００３５】図５に、前記Ｓ５００処理の暗号／復号化プログラム登録および削除処理の流れを示す。まず、受信データヘッダー部の暗号／復号化プログラムの登録（登録メモリ）または削除の領域を参照して、Ｓ５１０処理において、登録処理対象となる暗号／復号化プログラムの登録領域がＥＥＰＲＯＭ２４０かＲＡＭ２５０かを判定する。

【００３６】登録削除対象がＥＥＰＲＯＭ２４０内の場合は、Ｓ５２０処理において登録または削除の判定を行ない、登録要求の場合は、Ｓ５３０処理においてＥＥＰＲＯＭ２４０内の暗号／復号化プログラム管理データに受信データから暗号／復号化プログラムの管理データを作成しＥＥＰＲＯＭ２４０内に格納する。削除要求の場合は、Ｓ５４０処理において、Ｓ４００処理の結果を元にＥＥＰＲＯＭ２４０内の管理データと指定された暗号／復号化プログラム自体を削除する。

【００３７】登録削除対象がＲＡＭ２５０内の場合は、Ｓ５５０処理において、登録または削除の判定を行なう。登録要求の場合は、Ｓ５６０処理において、ＲＡＭ２５０内の暗号／復号化プログラム管理データに受信したデータから暗号／復号化プログラムの管理データを作成しＲＡＭ２５０内に格納する。削除要求の場合は、意識的に削除処理は実行せずに、ＲＡＭの揮発特性を使用してＩＣカード１００に対する電源供給が断たれたときにＲＡＭ２５０内から管理データを削除（揮発）させる。

【００３８】図６に、図３のＳ６００の暗号／復号化プログラム起動処理の流れを示す。、まず、対象となる暗号／復号化プログラムの識別子が例えば「Ｃ０３０１１」の場合、プログラム自体を「Ｃ０００００」プログラムで復号化するために、暗号／復号化プログラム暗号復号化処理Ｓ７００をコールする。

【００３９】図７に示すＳ７００処理では、Ｓ７１０処理で、復号処理のための暗号／復号化プログラムの識別子（復号処理の欄）の有無を判定する。例えば「Ｃ０３０１１」が指定されている場合は、「Ｃ０００００」で復号化する必要があるため、当該識別子を使用して暗号／復号化プログラム選択処理Ｓ４００をコールし、暗号／復号化プログラム管理データ情報を取得し、Ｓ７００処理を再帰的にコールする。

【００４０】再帰的にコールされたＳ７００処理では、指定された識別子「Ｃ０００００」の暗号／復号化プログラムを復号化する必要があるかどうかを、Ｓ７１０処理で判定する。「Ｃ０００００」の暗号／復号化プログラムは復号する必要が無いのでそのままリターンする。

【００４１】再帰的にコールしたＳ７００処理からリターンされると、Ｓ７１０処理において識別子「Ｃ０３０１１」の暗号／復号化プログラムは識別子「Ｃ０００００」によって復合化され、Ｓ６００処理へリターンする。

【００４２】Ｓ７００処理で復号化された識別子「Ｃ０３０１１」の暗号／復号化プログラムを使用して、Ｓ６１０処理において、受信データヘッダー部のデータ種別がデータで、復号化プログラムの識別子が「Ｃ０３０１１」を指定してある受信したデータの復号化処理を実行する。

【００４３】以後Ｓ３８０処理において受信したデータの参照、加工およびメモリ１１０への記憶、更新が可能になる。

【００４４】ＩＣカード１００の受信データのデータ種別がデータの場合は、ヘッダー部に格納された復号化プログラムの識別子に従い、暗号／復号化プログラム起動処理Ｓ６００をコールすることで、データの復号処理が実行される。

【００４５】さらに、ＩＣカード１００の受信データの

データ種別がデータの場合で、ヘッダー部に復号化プログラムの識別子が格納されていない場合は、ＩＣカード１００が受信したデータは復号化の必要がない。

【００４６】ＩＣカードから暗号化したデータを送信する場合は、Ｓ６００処理を使用し、暗号化対象データと暗号／復号化プログラムを指定し、Ｓ６００処理においてデータを暗号化した後で、データ送信処理Ｓ３２０において、図８の形式に従ったデータ形式に変換して入出力インタフェース（Ｉ／Ｏ）２２０を介して通信回線上にデータを送信する。

【００４７】本発明のＩＣカード１００に対して暗号／復号化プログラムの登録削除ならびにデータ送受信を外部情報処理装置から行なう場合は、図６、図７に記載した処理方式と図８に示したデータ形式に従った処理を行なうことで可能になる。

【００４８】上記の実施形態により、秘匿したいデータの暗号化または復号化処理は、ＩＣカード内に格納された暗号／復号化プログラムに依存することになり、さらに各ＩＣカード毎に異なる暗号／復号化プログラムを搭載することが可能になる。

【００４９】

【発明の効果】以上説明したように、本発明によれば、暗号／復号化プログラムを記憶させる手段と、暗号／復号化プログラムを起動させる手段と、暗号／復号化プログラム自体を外部の情報処理装置または他のＩＣカードに送受信する手段と、暗号／復号化プログラム登録削除手段とを、ＩＣカード内に備えるようにしているので、ＩＣカードから外部の情報処理装置または他のＩＣカードに暗号化したデータを送信する場合、送信するデータをＩＣカード内に記憶されている暗号／復号化プログラムを使用して暗号化し、暗号化したデータの送信時または事前に暗号化したデータを復号化するため暗号／復号化プログラムを送信先に送信し、データを受信した情報処理装置または他のＩＣカードは、受信した暗号／復号化プログラムを使用して受信した暗号化されたデータの復号化を行なうことが可能になる。これにより、各ＩＣカード毎に異なる暗号／復号化プログラムをＩＣカード内に保有することが可能になる。また、全てのＩＣカードの暗号／復号化プログラムを情報処理装置内で一括保有することを不要にする。

【００５０】またＩＣカード内に暗号／復号化プログラム自体を別の暗号化鍵または暗号化プログラムで暗号化する手段と、暗号化されたプログラムを暗号化した暗号化鍵に対応する復号化鍵または復号化プログラムで復号化する暗号／復号化プログラム暗号復号化手段を備えることで、ＩＣカードから送信する暗号／復号プログラム自体を暗号化することを可能にし、送信中の暗号／復号化プログラムの秘匿性を向上することを可能にする。

【図面の簡単な説明】

【図１】本発明のＩＣカード内に組込む手段のブロック図

【図２】本発明のＩＣカードを構成するハード機構のブロック図

【図３】図１における暗号／復号化プログラムおよびデータ送受信手段の処理フローチャート図

【図４】図１における暗号／復号化プログラム選択手段の処理フローチャート図

【図５】図１における暗号／復号化プログラム登録削除手段の処理フローチャート図

【図６】図１における暗号／復号化プログラム起動手段の処理フローチャート図

【図７】図１における暗号／復号化プログラム暗号復号化手段の処理フローチャート図

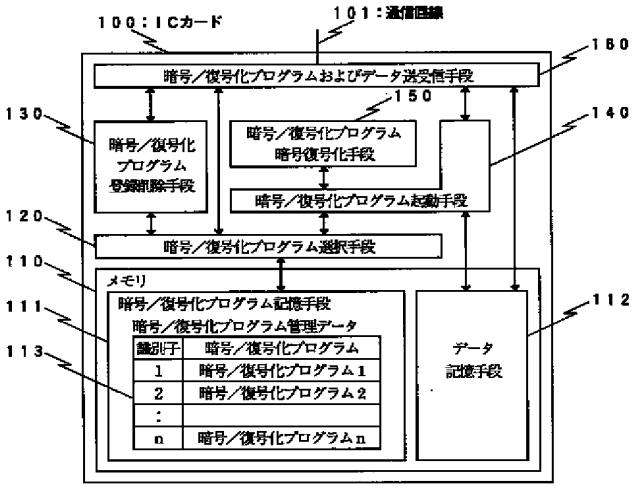
【図８】本発明のＩＣカードが送受信するデータ形式例を示す図

【図９】図１における暗号／復号化プログラム記憶手段内部に格納する暗号／復号化プログラム管理データの例を示す図

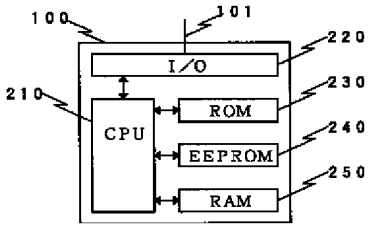
【符号の説明】

１００：ＩＣカード、１０１：通信回線（有線または無線の伝送路）、１１０：メモリ（ＥＥＰＲＯＭまたはＲＡＭを示す）、１１１：暗号／復号化プログラム記憶手段、１１２：データ記憶手段、１１３：暗号／復号化プログラム管理データ、１２０：暗号／復号化プログラム選択手段、１３０：暗号／復号化プログラム登録削除手段、１４０：暗号／復号化プログラム起動手段、１５０：暗号／復号化プログラム暗号復号化手段、１６０：暗号／復号化プログラムおよびデータ送受信手段、２１０：ＣＰＵ、２２０：入出力インタフェース（Ｉ／Ｏ）、２３０：ＲＯＭ、２４０：ＥＥＰＲＯＭ、２５０：ＲＡＭ。

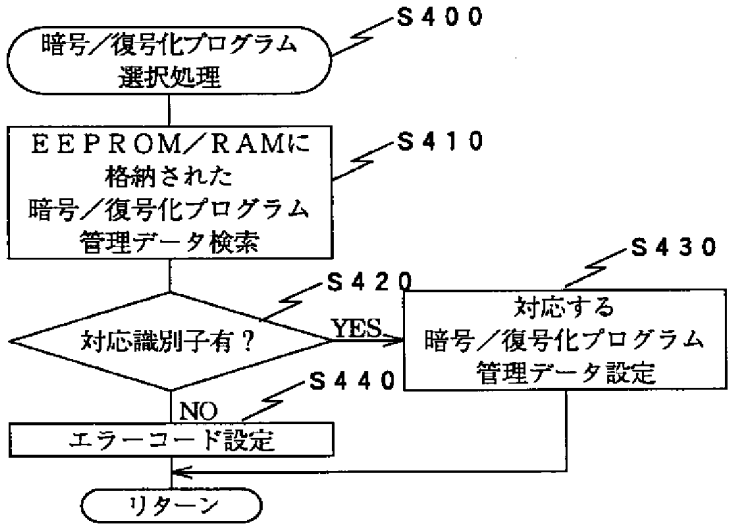
【図１】


100：ICカード
101：通信回線
暗号／復号化プログラムおよびデータ送受信手段
180
150
130
暗号／復号化プログラム登録削除手段
暗号／復号化プログラム暗号復号化手段
140
暗号／復号化プログラム起動手段
120
暗号／復号化プログラム選択手段
110
メモリ
111
暗号／復号化プログラム記憶手段
暗号／復号化プログラム管理データ
113
識別子
暗号／復号化プログラム
1
暗号／復号化プログラム１
2
暗号／復号化プログラム２
:
n
暗号／復号化プログラムｎ
データ記憶手段
112

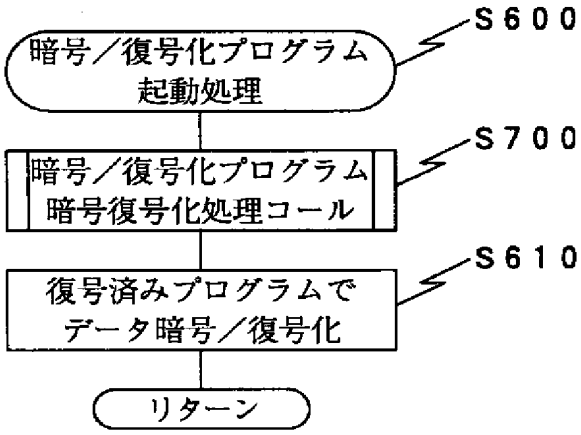
【図２】


100
101
220
I/O
230
210
CPU
ROM
240
EEPROM
250
RAM

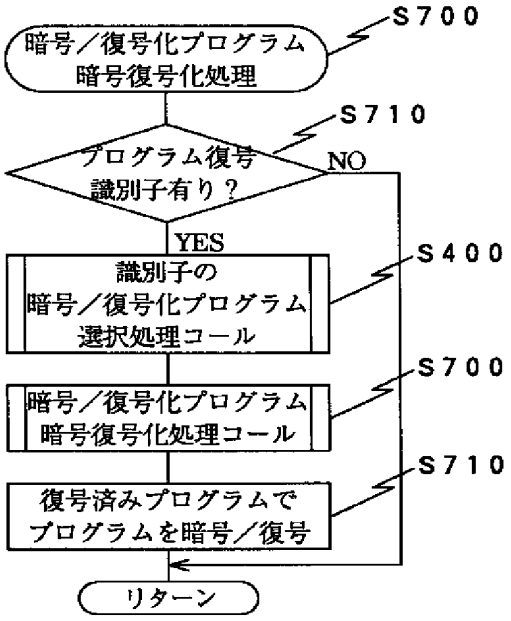
【図４】


S400
暗号／復号化プログラム選択処理
S410
EEPROM／RAMに格納された暗号／復号化プログラム管理データ検索
S420
対応識別子有？
YES
S430
対応する暗号／復号化プログラム管理データ設定
NO
S440
エラーコード設定
リターン

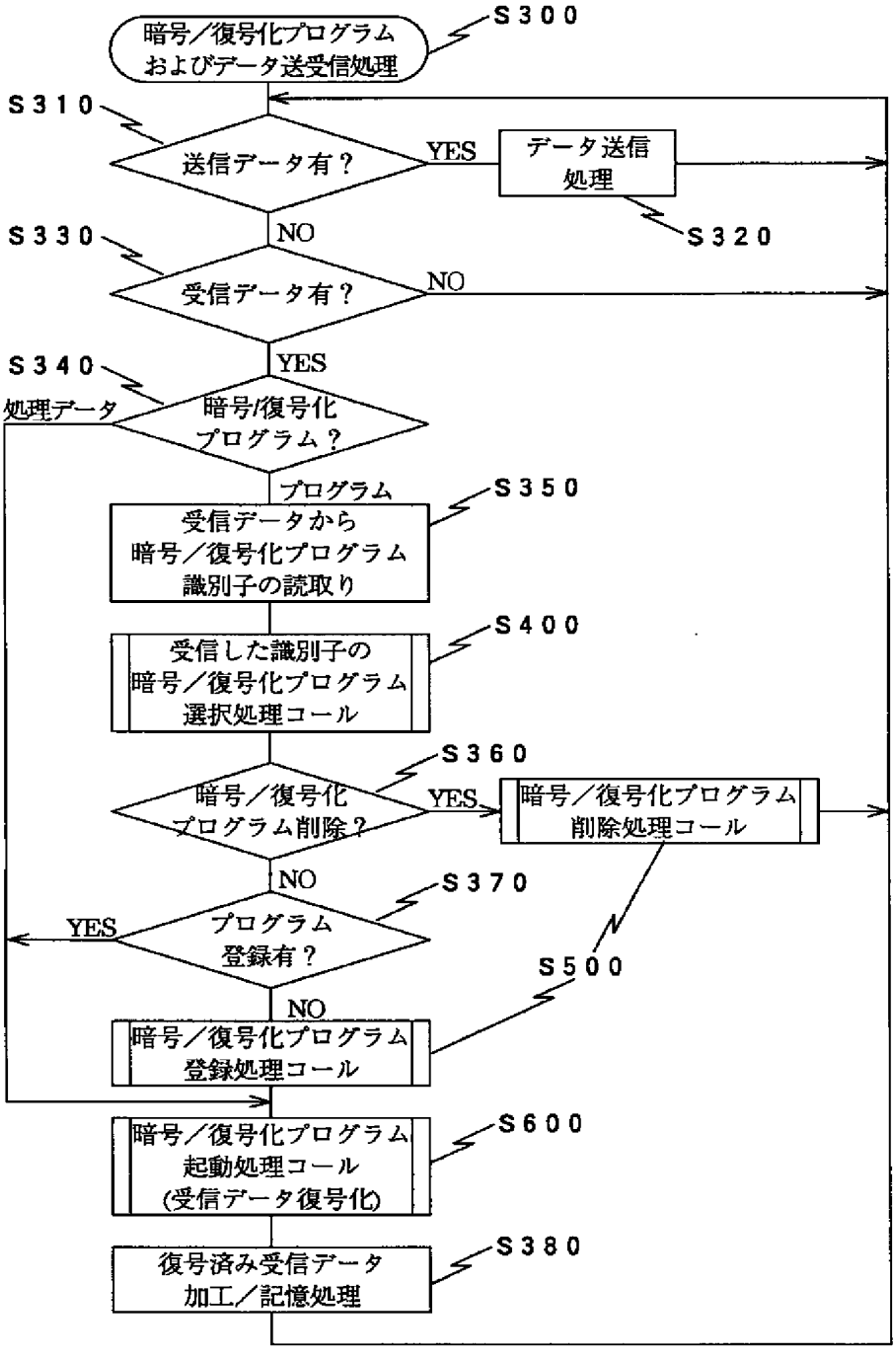
【図６】


S600
暗号／復号化プログラム起動処理
S700
暗号／復号化プログラム暗号復号化処理コール
S610
復号済みプログラムでデータ暗号／復号化
リターン

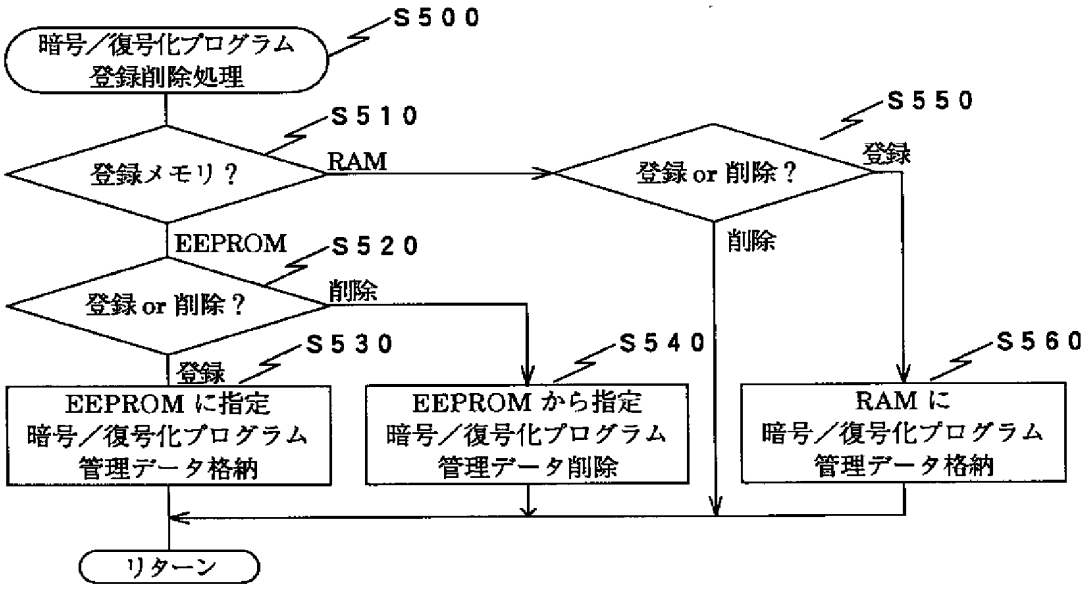
【図７】


S700
暗号／復号化プログラム暗号復号化処理
S710
プログラム復号識別子有り？
NO
YES
S400
識別子の暗号／復号化プログラム選択処理コール
S700
暗号／復号化プログラム暗号復号化処理コール
S710
復号済みプログラムでプログラムを暗号／復号
リターン

【図３】


暗号／復号化プログラム
およびデータ送受信処理
S300
S310
送信データ有？
YES
データ送信
処理
S320
NO
S330
受信データ有？
NO
YES
S340
処理データ
暗号/復号化
プログラム？
プログラム
S350
受信データから
暗号／復号化プログラム
識別子の読取り
S400
受信した識別子の
暗号／復号化プログラム
選択処理コール
S360
暗号／復号化
プログラム削除？
YES
暗号／復号化プログラム
削除処理コール
NO
S370
YES
プログラム
登録有？
S500
NO
暗号／復号化プログラム
登録処理コール
暗号／復号化プログラム
起動処理コール
(受信データ復号化)
S600
復号済み受信データ
加工／記憶処理
S380

【図５】



【図８】

ヘッダー部	データ種別			
	データの長さ			
	プログラム時	暗号／復号化プログラムの識別子	データ時	復号化プログラムの識別子
		暗号／復号化プログラムの復号処理用の識別子		－
		暗号／復号化プログラムの登録（登録メモリ）または削除		－
データ部	暗号／復号化プログラム または データ			

【図９】

識別子		暗号／復号化プログラム				
登録カードID	Ｎｏ	暗号化プログラム	復号化プログラム	復号処理		送信先登録メモリ
				登録カードＩＤ	Ｎｏ	
Ｃ０００	００	アドレス	アドレス	－	－	－
Ｃ００１	０１	アドレス	アドレス	Ｃ０００	００	ＥＥＰＲＯＭ
Ｃ００１	０２	アドレス	アドレス	Ｃ００１	０１	ＲＡＭ
：	：	：	：			
Ｃ０２０	１０	－	アドレス	－	－	－
Ｃ０３０	１１	－	アドレス	Ｃ０００	００	－
：	：	：	：			

DERWENT-ACC-NO: 2000-211440

DERWENT-WEEK: 200019

TITLE: Integrated circuit card for use with information processor, includes registration deletion unit which deletes encoding-decoding program after completion of decoding of predefined data

INVENTOR: OBANA M; OKUHARA S ; TAKEYABU H

PATENT-ASSIGNEE: HITACHI LTD[HITA]

PRIORITY-DATA: 1998JP-149147 (May 29, 1998)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE
JP 11338993 A	December 10, 1999	JA

APPLICATION-DATA:

PUB-NO	APPL-DESCRIPTOR	APPL-NO	APPL-DATE
JP 11338993A	N/A	1998JP-149147	May 29, 1998

INT-CL-CURRENT:

TYPE	IPC DATE
CIPP	G06K19/073 20060101
CIPS	G06K19/10 20060101

ABSTRACTED-PUB-NO: JP 11338993 A

BASIC-ABSTRACT:

NOVELTY - A memory (111) stores encoding-decoding program. An execution unit (140) executes stored program. When encoded data is transmitted to the data receiving element, the program communication unit (160) transmits the decoding program for decoding the predefined data. The registration deletion unit (130) deletes the encoding-decoding program after completion of the decoding of predefined data.

USE - Integrated circuit (IC) for use with information processor.

ADVANTAGE - Encoding-decoding program different for every IC card can be stored and hence avoids need for batch retention of encoding and decoding programs of all IC cards. Improves secrecy of encryption and decoding program during transmission using simple technique. DESCRIPTION OF DRAWING(S) - The figure depicts the block diagram of IC card. (111) Memory; (130) Registration deletion unit; (140) Execution unit; (160) Communication unit.

CHOSEN-DRAWING: Dwg.1/9

TITLE-TERMS: INTEGRATE CIRCUIT CARD INFORMATION PROCESSOR REGISTER DELETE UNIT ENCODE DECODE PROGRAM AFTER COMPLETE PREDEFINED DATA

DERWENT-CLASS: T01 T04 W01

EPI-CODES: T01-D01; T01-H01B3A; T04-K02; W01-A05A;

SECONDARY-ACC-NO:

Non-CPI Secondary Accession Numbers: 2000-158237

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the IC card which enciphers and decrypts data by the code and decoding processing based on a program.
[0002]
[Description of the Prior Art]The processing which enciphers data to keep secret, using an enciphering key as a technique for keeping data (it is also called "information".) secret conventionally is known. Since it cannot return to the state where it is decipherable if the key same once data is enciphered as the key used by encryption, or a specific decryption key is not used, it is possible to make data secret to those who own neither such an enciphering key nor the decryption key.
[0003]If an enciphering key and a decryption key are revealed, since data will be decoded, safety has been improved by enciphering and keeping it with another enciphering key to this enciphering key and decryption key.
[0004]As for the decoding processing for data encryption processing or a data decipherment, in such a system, it is common that a code/decoded program performs with an information processor. The privacy of data is improved because data is enciphered by this code/decoded program, and also even an enciphering key enciphers in order to improve safety. However, it is common for this the code / decoded program itself to be more nearly defenseless than the data itself. A third party's analysis of such a code/a decoded program will decode the enciphered data. Or also in a possibility of becoming possible, the third party has decoded all the enciphered data after that by altering the code / the decoded program itself, and adding a means to encipher with the enciphering key which the third party knows.
[0005]In order to perform encryption or decryption efficiently, without a third party altering this code/decoded program, in JP,9-6232,A. Encipher the code / the decoded program itself with

another enciphering key, and it stores in the nonvolatile memory in an information processor, When transmitting data from an information processor to an IC card, the enciphered code/decoded program are transmitted to the volatile memory in an IC card, After decrypting the program concerned in an IC card, it transmits to the volatile memory of an information processor, and the data encryption or decryption which transmits is performed using the decrypted code/decoded program.

[0006]

[Problem(s) to be Solved by the Invention]However, when using different code/decoded programs for every IC card in such a system, Since it was necessary to hold the code/decoded program as which all the IC cards were enciphered in the information processor which transmits and receives an IC card and data, the technical problem that a huge storage capacity was required occurred.

[0007]When transmitting the code/decoded program furthermore decrypted within the IC card to an information processor, a code/decoded program is in a defenseless state, and the technical problem that the possibility of disclosure of the code/decoded program under transmission is expanded occurs.

[0008]This invention does not have the necessity of carrying out package possession of the code/the decoded program of all the IC cards into an information processor, and an object of this invention is to provide the IC card which raised the privacy of the code/decoded program.

[0009]

[Means for Solving the Problem]A means by which this invention makes a code/decoded program memorize in order to attain the above-mentioned purpose, It has a means to start a code/decoded program, a means to transmit and receive the code / the decoded program itself to an external information processor or other IC cards, and a code / decoded program registration deleting means, in an IC card.

[0010]That is, IC card of this invention used by a system which enciphers transmitted and received data by a code and decoding processing based on a program is characterized by that an invention concerning claim 1 comprises the following.

The code / decoded program memory measure for memorizing encryption or a decoded program (it is henceforth described as a code/decoded program)

The code / decoded program starting means which starts the code/decoded program memorized by the code / decoded program memory measure, and uses encryption object data as code data, or uses decryption object data as decode data

The code / decoded program transmission and reception means which transmits and receives the code/decoded program for decoding enciphered data beforehand or simultaneous to data receiving origin when transmitting data enciphered by the code/decoded program

The code / decoded program registration deleting means which registers and deletes a

code/decoded program to a code / decoded program memory measure

[0011]In claim 1, as for an invention concerning claim 2, said code / decoded program memory measure memorize two or more said codes / decoded programs.
[0012]In an IC card which an invention concerning claim 3 equips with the code / the decoded program memory measure according to claim 2, It had a means to register and delete arbitrary code/decoded programs from two or more code/decoded programs, and the code / decoded program selecting means which starts arbitrary code/decoded programs in a code / decoded program starting means further.
[0013]It is an invention concerning claim 4 being provided with an identification device for identifying arbitrary code/decoded programs which are memorized in an IC card in the code / the decoded program selecting means according to claim 3, and specifying an identifier, It had the code / decoded program starting means which starts corresponding code/decoded program.
[0014]A means to encipher the code / the decoded program itself which indicated an invention concerning claim 5 to claim 1 in claims 1-4 by an another enciphering key or an enciphered program, It had the code / decoded program code decoding means decrypted by a decryption key or a decoded program corresponding to an enciphering key which enciphered an enciphered program.
[0015]A means by which an invention concerning claim 6 transmits arbitrary code/decoding programs from claim 1 via a communication line to an IC card and this IC card of any one statement of five, A registry request means into an IC card of the code/decoded program which transmitted, Use an information processor provided with a deletion request means of arbitrary code/decoded programs in an IC card, and between an IC card and an information processor or between different IC cards, They are the code/decoding system performing a data encryption and decryption which are transmitted and received via a communication line.
[0016]
[Embodiment of the Invention]Hereafter, an embodiment of the invention is described using a drawing.
[0017]Drawing 2 is a hard mechanism block figure which constitutes IC card 100 of an embodiment of the invention. This IC card 100 is provided with CPU210, the input/output interface (I/O) 220, ROM230, RAM250, and EEPROM240. ROM230 shows the nonvolatile memory which cannot perform renewal of a memory content, although read-out of a memory content is possible. Although read-out and updating of a memory content are possible for both RAM250 and EEPROM240, RAM250 shows the volatile memory which loses a memory content, when the current supply to IC card 100 is cut off, and EEPROM240 shows the nonvolatile memory which does not lose a memory content even if the current supply to IC

card 100 is cut off. [0018]Drawing 1 is a block diagram which has arranged each component for realizing this invention in IC card 100 shown in drawing 2. The memory 110 shows the storage area assigned in RAM250 of drawing 2, or EEPROM240. The code / decoded program memory measure 111 which memorizes the code/decoded program for decrypting the data enciphered or enciphered in data to make secret are assigned in the memory 110.
[0019]The data storage means 112 for memorizing the data processed within the data which IC card 100 received, or IC card 100 is assigned to field where the code / decoded program memory measure 111 in the memory 110 are another.
[0020]Each code/decoded program memorized in the code / decoded program memory measure 111 are managed with a code / decoded program management data 113. Drawing 9 is one example of a code / decoded program management data.
[0021]When choosing arbitrary code/decoded programs by the processing in IC card 100, a code / decoded program selecting means 120 chooses the specified code/decoded program by referring to a code / decoded program management data 113.
[0022]When arbitrary code/decoded programs which have already been registered into the code / decoded program memory measure 111 by registration, or the code / decoded program memory measure 111 in arbitrary code/decoded programs are deleted, The result of having chosen the specified code/decoded program by the code / decoded program selecting means 120 to origin. . Incorporate the code/decoded program which management data was registered into the code / decoded program management data 113 within a code / decoded program memory measure 111 by the code / decoded program registration deleting means 130, and was specified in the memory 110. Or the code/decoded program which management data corresponding from a code / decoded program management data 113 is deleted, and corresponds are deleted from the memory 110.
[0023]When starting arbitrary code/decoded programs within IC card 100, By starting the code/decoded program specified by the code / decoded program starting means 140 based on the result of having chosen the specified code/decoded program by the code / decoded program selecting means 120. The data encryption or decryption which is memorized in the data storage means 112 and which should be enciphered is performed.
[0024]When data [need / the code / the decoded program itself / to be decrypted] is stored in the code / decoded program starting means 140 in the code / decoded program management data 113 of the specified code/decoded program, After decrypting the code/decoded program specified by the code / decoded program code decoding means 150, it starts by the code / decoded program starting means 140. [0025]In IC card 100, data, or a code/decoded program is received from an external information processor, Or the data to the communication line 101 is transmitted [when transmitting data, or a code/decoded program to an external information processor] and received using the input/output interface (I/O) 220 by the code / decoded

program, and the data-transmission-and-reception means 160. [0026]In the block diagram of drawing 1, in a code / decoded program selecting means 120, the code / decoded program registration deleting means 130, the code / decoded program starting means 140, the code / decoded program code decoding means 150, and a row. A code / decoded program, and the data-transmission-and-reception means 160 are incorporated in ROM230 which is the nonvolatile memory in IC card 100, or EEPROM240.

[0027]Henceforth, an example of the encryption which uses IC card 100 of the embodiment shown in drawing 1 and drawing 2, and encryption data transfer is explained based on drawing 3 - 9.

[0028]Drawing 3 shows processing of the code / decoded program for receiving data from data transmission or the communication line 101 to the communication line 101 using the input/output interface (I/O) 220 of IC card 100, and the data-transmission-and-reception means 160. This processing supervises the existence of transmitted and received data by the decision processing of S310 and S330 in order to always enable registration of data transmission and reception, when IC card 100 is a run state.

[0029]The form of the data transmitted and received is shown in drawing 8. When there are received data, it is processing of S340 and the data type of the header of received data is judged. The information for judging that a data type is an enciphered program, a decoded program, or data is set up. If it is a code/decoded program, the identifier of a code/decoded program will be read in received data in S350 processing, and the existence of the code/decoded program corresponding to a specification identifier will be checked by S400 processing.

[0030]The flow of the code / decoded program selection process of S400 is shown in drawing 4. The identifier of the code/decoded program which received, and an identifier in agreement are searched with a code / decoded program selection process S400 from the code / decoded program management data 113 set up in EEPROM240 and RAM250. When a corresponding identifier is detected, the return of the code / the decoded program management data corresponding to (S420) and its identifier is carried out, when it is not able to detect, an error code is set up as unregistered, and a return is carried out to S400 processing call origin.

[0031]The code / decoded program management data 113 which becomes a retrieval object by S400 processing constitute form as shown in drawing 9. The identifier for identifying a code/decoded program comprises a number of the code/decoded program managed within card ID which registered the code/decoded program, and its card. The management data of a code/decoded program The stored address in IC card 100 of an enciphered program, The stored address of the decoded program in IC card 100, and the memory classification registered into IC card 100 (exception of EEPROM or RAM), And when the code / the decoded program itself need to be decrypted before executing the code/decoding program registered, it

comprises an identifier (column of decoding processing) of the code/decoded program used for the decryption.

[0032]In the example shown in drawing 9, if card ID of self-IC card 100 is set to "C001", The code / decoded program identifier registered by the self-IC card are two kinds, "C00101" and "C00102", (an identifier shall connect and express the registration cards ID and No), The identifier means that the code/decoded program which is "C00102" are enciphered by "C00101." A code / decoded program identifier "C02010" means that only the management data of the decoded program for decrypting data at the time of the data receiving from card ID "C020" is stored. A code / decoded program identifier "C00000" expresses the code/decoded program standardly registered into IC card 100 so that it can be used [all the / IC card]. A code / decoded program identifier "C00101", and "C03011" mean being enciphered by this "C00000" by which standard registration was carried out.

[0033]It returns to drawing 3 again and it is judged [which registers the code/decoded program which received from the receiving data-headers part by S360 processing based on the result searched with a code / decoded program, andSdata-transmission-and-reception processing S400 processing of 300 / or or] whether it deletes. In the case of a deletion request, after calling a code / decoded program deletion S500 and deleting a specification code / decoded program, repetition processing is performed from S310 which checks the existence of send data. In the case of a registry request, it judges whether the code/decoded program which received by S370 processing are already registered based on the result of S400 processing, and when unregistered, a code / decoded program registration processing S500 is called. When the specification code / decoded program is already registered by S370 processing, or when a code/decoded program is newly registered into the memory 110 by S500 processing, The code / decoded program starting processing S600 specified succeedingly are called, and decoding processing of the data which IC card 100 receives is performed succeedingly.

[0034]The data decrypted by S600 processing processes received data by S380 processing, and after it performs processing of making the memory 110 memorize etc., it carries out repeat execution from S310 processing.

[0035]The flow of the code / decoded program registration of said S500 processing, and deletion is shown in drawing 5. First, with reference to registration (registration memory) of the code/decoded program of a receiving data-headers part, or the field of deletion, the registered area of the code/decoded program used as a registration processing object judges EEPROM240 or RAM250 in S510 processing.

[0036]When the candidate for registration deletion is in EEPROM240, The judgment of registration or deletion is performed in S520 processing, in the case of a registry request, in S530 processing, the management data of a code/decoded program is created from received data to the code / decoded program management data in EEPROM240, and it stores it in

EEPROM240. In the case of a deletion request, in S540 processing, the code / the decoded program itself specified as the management data in EEPROM240 based on the result of S400 processing are deleted.

[0037]When the candidate for registration deletion is in RAM250, the judgment of registration or deletion is performed in S550 processing. In S560 processing, in the case of a registry request, the management data of a code/decoded program is created from the data received to the code / decoded program management data in RAM250, and it stores it in RAM250. Deletion makes management data delete from the inside of RAM250 intentionally in the case of a deletion request, without performing, when the current supply to IC card 100 is cut off using the volatile characteristic of RAM (volatilization).

[0038]The flow of the code / decoded program starting processing of S600 of drawing 3 is shown in drawing 6. When the identifier of the target code/decoded program is "C03011" first, in order to decrypt the program itself by "C00000" program, a code / decoded program code decoding processing S700 is called.

[0039]In the S700 processing shown in drawing 7, the existence of the identifier (column of decoding processing) of the code/decoded program for decoding processing is judged by S710 processing. For example, since it is necessary to decrypt by "C00000" when "C03011" is specified, a code / decoded program selection process S400 is called using the identifier concerned, a code / decoded program management data information is acquired, and S700 processing is called recursively.

[0040]In the S700 processing called recursively, it is judged by S710 processing whether it is necessary to decrypt the code/decoded program of the specified identifier "C00000." Since there is no necessity of decoding, the return of the code/the decoded program of "C00000" is carried out as it is.

[0041]If a return is carried out from the S700 processing called recursively, in S710 processing, decoding of the code/the decoded program of an identifier "C03011" will be carried out by the identifier "C00000", and a return will be carried out to S600 processing by it.

[0042]The code/decoded program of the identifier "C03011" decrypted by S700 processing are used, and the data type of a receiving data-headers part performs decoding processing of the received data as which the identifier of the decoded program specifies "C03011" by data in S610 processing.

[0043]Reference of the data received in S380 processing after that, processing and the memory to the memory 110, and updating are attained.

[0044]When the data type of the received data of IC card 100 is data, according to the identifier of the decoded program stored in the header, it is calling a code / decoded program starting processing S600, and decoding processing of data is performed.

[0045]When the identifier of the decoded program is not stored in the header by the case

where the data type of the received data of IC card 100 is data, the data which IC card 100 received does not have the necessity for decryption.

[0046]When transmitting the data enciphered from the IC card, After using S600 processing, specifying encryption object data, and a code/decoded program and enciphering data in S600 processing, In the data transmission processing S320, it changes into the data format according to the form of drawing 8, and data is transmitted on a communication line via the input/output interface (I/O) 220.

[0047]When performing registration deletion and data transmission and reception of a code/decoded program from an external information processor to IC card 100 of this invention, it becomes possible by performing processing according to the data format shown in mode of processing indicated to drawing 6 and drawing 7, and drawing 8.

[0048]It will depend for encryption or decoding processing of data to keep secret on the code/decoded program stored in the IC card, and the above-mentioned embodiment enables it to carry further different the code/a decoded program for every IC card.

[0049]

[Effect of the Invention]A means to make a code/decoded program memorize as explained above according to this invention, A means to start a code/decoded program, and a means to transmit and receive the code / the decoded program itself to an external information processor or other IC cards, Since he is trying to have a code / decoded program registration deleting means in an IC card, When the data enciphered from the IC card to an external information processor or other IC cards is transmitted, The data to transmit is enciphered using the code/decoded program memorized in the IC card, The information processor or other IC cards which transmitted the code/decoded program to the transmission destination in order to decrypt the data enciphered the time of transmission of the enciphered data or beforehand, and received data, It becomes possible to decrypt the enciphered data which was received using the code/decoded program which received. It enables this to hold different code/decoded program for every IC card in an IC card. It makes it unnecessary to carry out package possession of the code/the decoded program of all the IC cards within an information processor.

[0050]A means to encipher the code / the decoded program itself by an another enciphering key or enciphered program in an IC card, By having the code / decoded program code decoding means decrypted by the decryption key or decoded program corresponding to the enciphering key which enciphered the enciphered program. It makes it possible to encipher the code / the decoding program itself which transmits from an IC card, and makes it possible to improve the privacy of the code/decoded program under transmission.

[Translation done.]